INDEPENDENT INQUIRY
CHILD SEXUAL ABUSE

Information and Records Management Policy

For publication

IICSA Information and Records Management Policy Statement

IICSA staff are required to read and comply with this policy and also with IICSA Information Management procedures in order to ensure compliance with relevant information legislation.

What is relevant information legislation

Information legislation means the:

1) The Inquiries Act 2005
2) The Inquiry Rules 2006
3) Data Protection Act 2018 & UK GDPR
4) Public Records Act 1958

The Independent Inquiry into Child Sexual Abuse is subject to the Inquiries Act 2005 and the Inquiries Rules 2006, which require the chair to ensure that the record of the Inquiry is "comprehensive and well-ordered".

Other relevant legislation includes the UK GDPR , Data Protection Act 2018, the Public Records Act 1958 and, once the Inquiry has closed, the Freedom of Information Act 2000.

These statutes assign a legal responsibility to all staff to value, protect and store information so that it is of use to the business and creates a publicly available archive at the end of the Inquiry. By following this policy, staff will be able to deliver on this responsibility.

What is our Objective?

To ensure that we comply with legislation by:

1) Requiring that information, particularly that relating to identifiable individuals, is handled in line with IICSA's Privacy Statement.

2) Requiring staff to be responsible for filing information and records in corporate repositories where access can be controlled and sharing is undertaken with due consideration for content and sensitivity;

3) Identifying and organising a full and proportionate record of the Inquiry so that it survives;

4) Depositing the selected records of the Inquiry with The National Archives for permanent preservation or with an appropriate government department to be retained for a stated period of time, having been reviewed for disclosure under the Freedom of Information Act.

5) Ensuring that all information which is not selected for permanent preservation has been

securely deleted and destroyed.

Scope of this policy; business information and evidential material

Business information includes any document which is generated by the Inquiry and its teams during the course of their work and does not include evidential material supplied by providers of information (PoIs).

Business information should be held in digital format; significant emails are stored with other information and must not be stored solely in personal mailboxes.

It is important that business information is captured so that important records survive which capture the following:

> **A decision and how that decision was reached** (e.g. minutes of meetings, correspondence prior to and after the meeting that result in a decision being made and/or an action taken forward)
> **How procedures work** (e.g. work plans, standard operating procedures and changes to them), or
> **Contractual/purchasing arrangements** (e.g. service delivery contracts, purchase orders).

Additionally large numbers of evidential documents have been received from contributing organisations and individuals. These will be managed so that information is available only to those who need to access and share it, allowing them to work securely and effectively.

Sharing and handling of data

The Inquiry has many stakeholders and it will sometimes be necessary to share data with them. This will be done securely in line with data protection legislation.

The Inquiry is registered with the Information Commissioner's Office as a data controller because the Inquiry decides how both personal and sensitive personal data are processed. Given the nature of the subject matter that the Inquiry covers, staff will be advised how to take appropriate care when handling personal data to ensure that breaches of data protection legislation and Inquiry policies do not occur.

Personal data will not be shared with others unless the Inquiry panel has explicitly stated that it will do so; for example, allegations made through correspondence will be passed to the police as stated on the Inquiry's website.

No personal data of living individuals will be made public by the Inquiry without written consent.

Requests under the Freedom of Information Act

The Inquiry is not a public authority for the purposes of the Freedom of Information Act (FoI) 2000. Therefore, while the Inquiry is in the course of its work and before its conclusion, the Act does not strictly apply and any requests for information made under the Act will not be considered.

However, to balance this approach the Inquiry will operate on a presumption of openness and transparency. As much information as possible will be provided publicly, mainly through the Inquiry's website.

The Home Office and other public bodies may receive FoI requests about the work of the Inquiry. Arrangements will be made for the Inquiry to assist with responses to those requests.

Security of information

The security of information that the Inquiry gathers, holds and has access to is fundamental to its integrity. It will also assist in delivering the success of the Inquiry. Therefore, information must be protected and kept secure.

As well as document handling and clear desk policies in the office and off-site, staff must observe the need for security when working from home, by not removing material from the office environment, when working on public transport and in discussions about the work of the Inquiry with family, friends, and other third parties including officials from government departments.

As far as possible, digital documents will not be printed; where it is necessary to print, paper copies will be placed in shredding cabinets as soon as they are no longer needed and the clear desk policy will be adhered to at all times i.e. no papers left unattended on staff desks, and all papers cleared away at the end of day and either locked away or shredded.

Staff will be provided with secure devices and training on data handling. Staff are required to not email any information relating to the Inquiry to any personal devices or email accounts.

Retention and disposal of information

IICSA is obliged by law to manage its records effectively and to retain them only as long as necessary to meet business needs and statutory requirements. To comply with this requirement, the Information Management function allocates retention periods to our records, to ensure that records for each function are retained for the appropriate length of time, but no longer.

Significant dialogue and decision making now often takes place by email. Storing such emails in personal mailboxes means they cannot be shared appropriately with other colleagues.

Emails need to be managed, so that

- substantive emails should be saved to a shared folder in the corporate file plan
- retention schedules will be applied to all contents of folders in the corporate file plan

- ephemeral emails which will not become a matter of record should be deleted as soon as possible, and personal email accounts will not be retained

At the end of the retention period, records will either be destroyed, or will be transferred to The National Archives or to a department of Her Majesty's Government. Before transfer, the records, regardless of format, will be reviewed and any FoI exemptions identified and records appropriately marked or redacted.

Roles and Responsibilities

- **Alexis Jay, as the Chair of the Inquiry,** has ultimate responsibility for the Inquiry's records and must ensure that appropriate functions, policies and procedures are in place to support the Inquiry during its lifetime and to produce a permanent record once the final report has been published

- **All members of the Inquiry team** must ensure that comprehensive records are kept of the Inquiry's activities, are required to work in the corporate information systems so that records are available to others, and that records are managed in line with our retention and disposal policy.

- **The information management function** supports compliance with relevant legislation and standards, oversees the corporate information system, assists in collating evidence and provides advice on information management and security.

- **The Deputy Chief Operating Officer acts as Senior Information Risk Owner (SIRO)** and is responsible for managing the risks of poor information management.

Compliance

This policy applies to all staff, consultants and contractors. Third party suppliers and anyone providing a service on IICSA's behalf should also be aware of the content of the policy.

Audit Logging and Monitoring

Management reserves the right to monitor and audit any and all use of our information resources, whether that use is business or personal. The outcomes of monitoring and audit activities is used to identify suspicious activity which could lead to the confidentiality, integrity and the availability of our information resources coming under threat therefore:

- User activity shall be monitored, logged and log files kept until no longer required in line with data protection laws;
- Where unacceptable activity, unlawful or illegal activity is detected, the individual issued with the account and / or computer equipment assigned to them shall be held culpable unless they can prove otherwise;

- logs shall only be made available to authorised personnel;
- logs shall be used internally to pursue disciplinary action;
- logs shall be handed to external entities if requested by law to pursue legal proceedings.

Policy Information

About this policy:

- any deviation or exceptions to the clauses within this policy, will be documented, reviewed and authorised by all relevant parties before exceptions are permitted;
- It will be supplemented with other policies to further mandate information security controls;
- It will be reviewed annually or when there are changes to the organisation to determine whether all aspects of the policy are up to date and applicable in the current business environments, and revised as necessary.
- Will be referred to when investigating any suspected violations reported by an individual. During the investigation it may be recommended to enforce disciplinary action in accordance with the organisation conduct, policies, or applicable laws. Sanctions may include one or more of the following:
    - suspension or termination of access;
    - disciplinary action up to and including termination of employment;
    - civil or criminal penalties;
    - or any combination of the above.